UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/661,734	09/12/2003	Donald Fedyk	120-279	8301

34845 7590 05/23/2008
Anderson Gorecki & Manaras LLP
33 NAGOG PARK
ACTON, MA 01720

EXAMINER	
RECEK, JASON D	

ART UNIT	PAPER NUMBER
2142	

NOTIFICATION DATE	DELIVERY MODE
05/23/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

handerson@smmalaw.com
officeadmin@smmalaw.com
cmorrissette@smmalaw.com

Office Action Summary	Application No.	Applicant(s)	
	10/661,734	FEDYK ET AL.	
	Examiner	Art Unit	
	JASON RECEK	2142	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 February 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-13* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-13* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *11 February 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This is in response to the amendment filed on February 11th 2008 which concerns application 10/661,734.

Status of Claims

Claims 1 and 3-13 are pending, claims 2 and 14-17 have been cancelled.

Claims 1 and 3-13 are rejected under 35 U.S.C. 103(a).

Claims 7-9 are rejected under 35 U.S.C. 101.

Response to Arguments

1. Applicant's arguments, see pg. 6-10, filed 2/11/08, with respect to the drawing objections, specification objections, claim objections and 112 rejections have been fully considered and are persuasive. The drawing objections, specification objections, claim objections and 112 rejections have been withdrawn.

2. Applicant's arguments with respect to the 101 rejections have been fully considered but they are not persuasive. Claim 7 recites a "network device", in the specification (paragraph 48) it is stated that this apparatus may be implemented as software. See rejection below.

3. Applicant's arguments with respect to the rejection(s) of claim(s) 1-3, 7 and 9-13 under 35 U.S.C. 102(e) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Hanzlik and Suzuki et al. U.S. 6,891,793 B1. See Below.

4. Applicant's arguments regarding the 103 rejections have been fully considered but they are not persuasive. Applicant merely argues the claims depend from an allowable claim, this is not persuasive since the claims do not currently depend from an allowable claim.

Claim Rejections - 35 USC § 101

5. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 7-9 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claim 7 recites "a network device". It is clear that a network device is not a process nor a composition of matter. A network device may be a machine or manufacture however in light of the specification (paragraph 48) a network device can be interpreted as being solely functional descriptive material (i.e. software). Functional descriptive material is non-statutory unless it is recorded on a computer readable medium that enables it to become structurally and functionally related (MPEP 2601.01). The claim does not recite any tangible physical elements that would exclude the claim

from being interpreted as software per se. Thus, the claim is neither directed towards a machine or a manufacture, but rather towards non-statutory subject matter.

Claims 8-9 do not recite any limitations that would render the claims statutory, therefore they are also rejected since they depend from a rejected claim.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1, 3, 7 and 9-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanzlik et al. US 2004/0044891 A1 in view of Suzuki U.S. 6,891,793 B1.

Regarding claim 1, Hanzlik discloses, "A method of securing communication between at least two members of a group" as a system and method for secure group communications (pg. 2, [0024]) through the implementation of a Virtual Private Group (VPG) communication system (paragraph 27), "wherein each member is an autonomous system [i.e. a collection of systems or devices operating under a single routing policy or domain, therefore able to communicate with one another without the use of the public backbone] comprising one or more network devices" as the capability for group members to exist behind a Network Address Translation (NAT) device (pg. 2,

[0028]) and capability for interdomain VPG's which are groups having members from different autonomous systems (paragraph 53), "forwarding, to at least one member of the group, a group security association [i.e. a set of information that defines how a group communicates securely, generally including policy and keys for securing communications] corresponding to the group" as sending a copy of the security policy, as well as a set of shared encryption keys and a membership key, from a policy server to the group nodes, where this information is used to secure group communications (pg. 4, [0043]), "receiving, from the at least one member of the group, route information enabling communication with each of the one or more network devices of the autonomous system corresponding to the member" as a management feature of the policy server, which manages group membership within its security domain (paragraph 41), each node has an identifier which may be an IP address (paragraph 59), when a node first contacts the policy server, its IP address (or that of the NAT device it is behind) is recorded when the node is authenticated (pg. 7, [oo75]).

Hanzlik also discloses "identifying at least one other member of the group" as creating a VPG membership list on the policy server, then adding members to that list and establishing secure connections between the policy server and the member nodes (pg. 5, [0060]), "reflecting the route information received from each member of the group to the at least one other member of the group" as sending the membership list from the policy server to each of the group members, (Pg. 5, [0061]) where the membership list presents group members by IP address and is applied to incoming and outgoing packets (pg. 4, [0043]) and "including the step of securing the route information using

the group security association" as establishing secure communications between the policy server and each node using one of the keys sent from the policy server to the node (pg. 4, [0042]). Encryption keys sent from the policy server to the group members are used to secure all communications, and include keys used to communicate with the policy server (pg. 4, [0043]).

Hanzlik does not explicitly disclose "the route information identifying a border router that should be used as the next hop to the at least one member of the group" however this generally known in the art and is explicitly taught by Suzuki as system where routing information is sent to end nodes (col. 1 ln. 40), the routing information identifies a path that includes what the next hop is, in this example it is a switch which is synonymous with a router (col. 1 ln. 30-59).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hanzlik by providing detailed route information as taught by Suzuki for the purpose communication. In order to transfer data (i.e. communicate) a device must know the destination, by providing directions to the destination (route information) the device will be able to communicate.

Regarding claim 3, Hanzlik discloses "further comprising the step of receiving a registration request from the at least one member of the group" as the initial contact by

a node asking for a VPG table (pg. 7, [0075]), which includes the IP addresses and security association data for other members of the VPG (pg. 7, [0070]).

Regarding claim 7, Hanzlik discloses "A network device for providing secure communications between at least two members of a group over a backbone network" as the policy server and VPG, as discussed above in the analysis of claim 1 (paragraphs 27, 41), "security association logic for forwarding a group security association of the group to the at least two members of the group" as a function of the policy server, as discussed above in the analysis of claim 1 (paragraph 42), "route reflection logic, for identifying at least one of the at least two members of the group, receiving routing information for the at least one of the two members of the group, ... securing the routing information for the at least one of the two members of the group using the group security association and for forwarding the secured routing information to another one of the at least two members of the group" as another function of the policy server, as discussed above in the analysis of claim 1 (paragraphs 42-43).

Hanzlik does not explicitly disclose "the route information identifying a border router that should be used as the next hop to the at least one member of the group" however this generally known in the art and is explicitly taught by Suzuki as system where routing information is sent to end nodes (col. 1 ln. 40), the routing information identifies a path that includes what the next hop is, in this example it is a switch which is synonymous with a router (col. 1 ln. 30-59).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hanzlik by providing detailed route information as taught by Suzuki for the purpose communication. In order to transfer data (i.e. communicate) a device must know the destination, by providing directions to the destination (route information) the device will be able to communicate.

Regarding claim 9, Hanzlik discloses "The device of claim 7 wherein the functionality for identifying at least one of the two members of the group includes a list of members of the group" as a VPG membership list, as discussed in the analysis of claim 1 (paragraph 42).

Regarding claim 10, Hanzlik discloses "A method for communicating securely by one member of a group of network devices with at least one other member of the group of network devices over a network backbone" as discussed above in the analysis of claim 1 (paragraph 27), "receiving, at the one member, a group security association corresponding to the group" as discussed above in the analysis of claim 1 (paragraph 60), "forwarding, by the one member to the at least one other member of the group, routing information for the one member" as discussed
above in the analysis of claim 1 (paragraphs 43, 61) and "the routing information being secured using the group security association of the group" as discussed above in the analysis of claim 1 (paragraph 42).

Hanzlik does not explicitly disclose "the route information identifying a border router that should be used as the next hop to the at least one member of the group" however this generally known in the art and is explicitly taught by Suzuki as system where routing information is sent to end nodes (col. 1 ln. 40), the routing information identifies a path that includes what the next hop is, in this example it is a switch which is synonymous with a router (col. 1 ln. 30-59).

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Hanzlik by providing detailed route information as taught by Suzuki for the purpose communication. In order to transfer data (i.e. communicate) a device must know the destination, by providing directions to the destination (route information) the device will be able to communicate.

Regarding claim 11, Hanzlik discloses "including the steps of:
receiving, at the one member, routing information associated with the at least one other member of the group, wherein the routing information associated with the at least one other member of the group is secured using the group security association of the group" as receiving a member list with IP addresses of other members, as discussed above in the analysis of claim 1 (paragraphs 43, 61).

Regarding claim 12, Hanzlik discloses "the steps of restoring the routing information associated with the at least one other member of the group using the group security association of the group" as the inherent result of receiving information from the policy server via a secure connection. Hanzlik states that "VPG nodes receive group membership information, and other VPG parameters, from [the] policy server," and that they "use this information to encrypt and decrypt traffic," (pg. 4, [0043]).

Hanzlik also discloses "securing a packet for transmission to the at least one other member of the group using the group security association to provide a secured packet" as the step where a member uses the security policy and group membership keys to encrypt data transmitted to another member node (pg. 5, [0053]) and "forwarding the secured packet to the at least one other member using the restored routing information" as the step where the member node applies the group membership list to all packets being sent or received (pg. 4, [0043]).

Regarding claim 13, Hanzlik discloses "forwarding includes building a tunnel [i.e. a secure connection characterized by the use of a key to encrypt and decrypt data transferred between two points] to the at least one other member of the group using the restored routing information and the group security association" as the use of the membership list and group keys, as discussed above in the analysis of claim 12, for symmetric encryption (pg. 3, [0034]).

8. Claims 4-6 and 8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hanzlik and Suzuki in view of Mukherjee et al. US 2004/0006708 A1.

Regarding claim 4 Hanzlik does not explicitly disclose "the registration request includes a list including the at least one other member of the group" however this is taught by Mukherjee as a registration process where the "subscriber identifies a group of users authorized" and states this information may be provided in the form of a list of members (Mukherjee, pg. 3, [oo4o]).

It would be obvious to one skilled in the art to modify Hanzlik to include populating the member list, once created on the policy server (pg. 5, [0060]), using a member list information provided by a member node when first connecting to the policy server, allowing a member node the authority to determine who is an authorized member (paragraph 48).

Regarding claim 5, Hanzlik does not explicitly disclose "wherein the step of identifying the at least one other member includes the step of forwarding a request for routing information to the at least one other member, the request including an identifier for the group" however this is taught by Mukherjee as an invitation sent to a second member, where the invitation is simply a mechanism used to notify the second user of the VPN set up by the first user. To join, the second user must respond to the invitation

(Mukherjee, pg. 5, [0055]). The invitation is effectively the request for routing information, as the session cannot be established without a response.

It would be obvious to one skilled in the art to modify Hanzlik to include populating the member list, once created on the policy server (paragraph 60), by sending out a request for routing information for members of an identified or named group, making the process more automated and therefore easier to use (Mukherjee, pg. 6, [0076]).

Regarding claim 6, Hanzlik does not explicitly disclose "wherein the step of identifying includes the step of auto-discovering the at least one other member of the group in response to the registration request by issuing a request for routing information to other devices in the network, the request for routing information including an identifier for the group" however this is taught by Mukherjee as "Augmenting the P2P-VPN with automatic network configuration procedures can provide easy networking to users without much knowledge about networking," (pg. 6, [0076]).

It would be obvious to one skilled in the art to modify Hanzlik to determine group members automatically, using auto-discovery means that are well known in the art, to populate the member list (paragraph 60) as one step in automatic configuration of a network, for the reasons disclosed by Mukherjee (i.e. ease of use for non-network savvy users).

Regarding claim 8, Hanzlik does not disclose "wherein the functionality for identifying at least one of the two members of the group is auto-discovery logic" however this is taught by Mukherjee (paragraph 76) as discussed in the rejection of claim 6.

It would be obvious to one skilled in the art to modify Hanzlik by adding a well-known auto-discovery means to populate determine other members of a group, where auto-discovery logic is one of the auto-discovery means well known in the art. Auto-discovery is not only well known, it also yields predictable results.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Thubert et al. U.S. 7,190,678 B2 discloses sending routing information in a message. The message includes border router information.

10. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JASON RECEK whose telephone number is (571)270-1975. The examiner can normally be reached on Mon - Thurs 8:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jason Recek/
Examiner, Art Unit 2142

(571)-270-1975

/Andrew Caldwell/
Supervisory Patent Examiner, Art Unit 2142